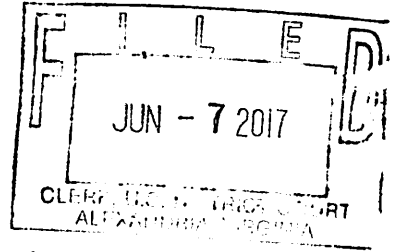


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 1:17-SW-311

VEHICLE IDENTIFIED AS A BLACK-COLORED FORD
SEDAN WITH VIRGINIA LICENSE PLATE WSK-6908
AND VIN 3FA6P0LUXDR225476

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1030(a)(2)(C)	Access of a Protected Computer without Authorization

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Colleen E. Garcia

Applicant's signature

Seunghyun Eom, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 06/07/2017

/s/ JFA
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Hon. John F. Anderson, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is the vehicle identified as a black-colored 4-door sedan with Virginia license plate WSK-6908 and VIN 3FA6P0LUXDR225476 located at 7510 Chancellor Way, Springfield, Virginia, 22153, further described as a single-family home with a detached carport. The residence has a green mailbox located at the curb to the left of the driveway. The curb is also marked with "7510" to the left of the driveway. The house has vertical beige-colored siding with brown-colored trim and brick. There are three (3) windows on the front of the house and a white-colored double-door for the front entrance.



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 1343 (Wire Fraud) and 1030(a)(2)(C) (Access of a Protected Computer without Authorization), those violations involving AHKTER and occurring after December 27, 2016 including:
 - a. Records and information relating to Victim Company 1, to include training certifications issued to AKHTER by Victim Company 1;
 - b. Records and information relating to the e-mail accounts munibee@hotmail.com and hirempire@gmail.com;
 - c. Records and information relating to malicious software;
 - d. Records and information relating to Victim 1, Victim 2, or Victim 3.
2. Computers or storage media used as a means to commit the violations described above, including downloading stolen banking credentials or stolen credit card information in violation of 18 U.S.C. § 1030(a)(2) and purchasing goods online using stolen credentials or credit card information in violation of 18 U.S.C. § 1343 (Wire Fraud).
3. For any computer, cell phone, smart phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of virtual environments or alternate operating systems used to obfuscate AKHTER's activities through the lack of monitoring software;
- c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- d. evidence of the lack of such malicious software;
- e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- f. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- g. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - i. evidence of the times the COMPUTER was used;
 - j. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - l. records of or information about Internet Protocol addresses used by the COMPUTER;
 - m. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - n. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media

that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

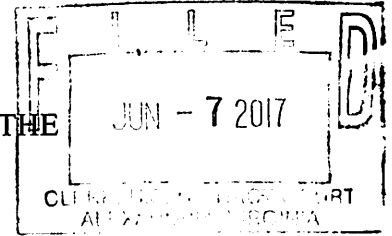
The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR A SEARCH WARRANT FOR THE
VEHICLE IDENTIFIED AS A BLACK-
COLORED 4-DOOR FORD SEDAN WITH
VIRGINIA LICENSE PLATE WSK-6908
AND VIN 3FA6P0LUXDR225476 LOCATED
AT 7510 CHANCELLOR WAY,
SPRINGFIELD, VIRGINIA 22153

Case No. 1:17SW311

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Seunghyun Eom, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the vehicle identified as a black-colored 4-door sedan with Virginia license plate WSK-6908 and VIN 3FA6P0LUXDR225476 located at 7510 Chancellor Way, Springfield, VA 22153, hereinafter "VEHICLE," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Criminal Computer Intrusion Squad of the Washington Field Office. I have been employed by the FBI for over 8 years. As a Special Agent of the FBI, I am authorized to investigate and

focus on crimes involving computer intrusions, Internet fraud, and identity theft, including violations of 18 U.S.C. §§ 1343 (Wire Fraud) and 1030(a)(2)(C) (Access of a Protected Computer without Authorization) .

3. The vehicle described in Paragraph 1 and in Attachment A are to be searched for evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 1343 (Wire Fraud) and 1030(a)(2)(C) (Access of a Protected Computer without Authorization). Such evidence, fruits, and instrumentalities are more particularly described in Attachment B to this affidavit.

4. The Federal Bureau of Investigation (FBI) and other law enforcement agencies are investigating Muneeb Akhter ("AKHTER") for believed Wire Fraud and Access of a Protected Computer without Authorization in violation of:

- a. 18 U.S.C. § 1343 (Wire Fraud): "[D]evising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmit[ing] or caus[ing] to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice."
- b. 18 U.S.C. § 1030(a)(2)(C) (Access of a Protected Computer without Authorization): "[I]ntentionally access[ing] a computer without authorization or exceeds authorized access, and thereby obtain[ing] information from any

protected computer.”

5. The facts and information contained in this affidavit are based upon my training and experience, participation in this and other investigations, personal knowledge, and observations during the course of this investigation, as well as the observations of other law enforcement officers and individuals involved in this investigation. All observations not personally made by me were related to me by individuals who made them or were conveyed to me by my review of the records, documents, and other physical evidence obtained during the course of the investigation.

6. This affidavit is only meant to contain information necessary to support probable cause for the requested search warrant and is not intended to include each and every fact observed by me or known to the government.

BACKGROUND

1. In 2014 and 2015, AKHTER secretly installed computer code on a victim company's computer that would allow him and his co-conspirators to steal information, including compromised credit cards, along with the names, addresses, phone numbers, and email addresses of the identity theft victims. AKHTER accessed the computer remotely, using his

personal laptop. AKHTER and his co-conspirators then made purchases via the Internet on multiple vendors' websites, using the stolen information.¹

2. On June 26, 2015, AKHTER pleaded guilty to six counts of a Criminal Indictment charging him with: Count One—conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1343 and 1349; Count Two—conspiracy to access a protected computer without authorization, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i)-(iii) and 371; Count Seven—access of a protected computer without authorization, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i), (iii); Count Eight—conspiracy to access a government computer without authorization, in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and (c)(2)(B)(i)-(iii) and 371; Count Ten—making a false statement in violation of Title 18, United States Code, Section 1001(a)(2); and Count Twelve—obstruction of the due administration of justice, in violation of Title 18, United States Code, Sections 1503 and 3147(1).

3. AKHTER began his prison sentence on October 26, 2016, and he was released from prison on December 27, 2016.

¹ When contacted by a Washington Post reporter in July 2014 regarding a search warrant for his residence, AKHTER deleted information from his computer and cell phone. When the search warrant was executed on his house and vehicle, a computer was located in his vehicle.

4. Following his release, AKHTER was placed on supervised release until December 27, 2019. The standard conditions of his release prohibited him from committing any additional crimes. The special conditions of release required the installation of computer monitoring software on any computer to which he had access. Senior U.S. Probation Officer Bethany Erding also instructed AKHTER to notify her of all computers and smart phones he used, to refrain from using additional operating systems without her knowledge, and to report all email addresses he used.

PROBABLE CAUSE

5. On May 17, 2017, the U.S. Attorney's Office, Eastern District of Virginia, was notified that the owner of Victim Company 1 had reported that AKHTER was still scamming people. After speaking with the owner, Senior Probation Officer Bethany Erding learned from the owner of Victim Company 1 that AKHTER registered for a training class provided by Victim Company 1. However, the class fee was charged to a PayPal account in the name of Victim 1 on Still Meadow Lane in West Bloomfield, MI. AKHTER attended the training from April 7, 2017 to April 8, 2017 and received a certification. Later, Victim Company 1 was notified by PayPal that Victim 1 had filed a complaint with PayPal, and that PayPal would not be paying the \$1300 class fee to Victim Company 1. Therefore, Victim Company 1 suffered a loss of \$1300.

6. Upon further review of the computer monitoring software, the U.S. Probation Office has seen Order Confirmation Emails sent to email addresses controlled by AHKTER and accessed while under computer monitoring.

- a. Amazon purchase confirmations have been emailed to email addresses accessed by AKHTER. The Amazon purchases were made in the name of Victim 2.
 - i. The receipt email address is munibee@hotmail.com.
- b. SAKS purchase confirmations have been emailed to email addresses accessed by AKHTER. The SAKS purchase was made in the name of Victim 3 on Breton Court in Reston, VA.
 - i. The receipt email address is hirempire@gmail.com. Internet searches indicate that AHKTER is the CEO of Hire Mpire.

7. After additional review of the computer monitoring software, Officer Erding saw that there was a nine-day gap in the computer monitoring, during which time there were no keystrokes made or websites accessed. According to RemoteCOM, which administers the computer monitoring program, if the computer is on, the monitoring will report every keystroke made and website accessed. Because there was a nine-day gap in monitoring, it is believed that the monitored computer was off during that time. However, Order Confirmation emails sent to emails controlled and accessed by AHKTER show Amazon purchases were made during the nine-day gap in monitoring.

8. For AHKTER to engage in online activity that is not captured by the computer monitoring software, he would have accessed an unmonitored device and/or accessed a virtual operating system that was not being monitored.

9. On June 2, Officer Erding conducted a surprise home inspection at AKHTER's residence. She saw multiple external hard drives and thumb drives in AKHTER's bedroom, which were contraband under the terms of his supervised release.

10. She also found a box of cell phones, including smart phones, in what used to be his mother's bedroom.² Because AHKTER had been prohibited from keeping these phones, AHKTER's mother had previously told Officer Erding that she (his mother) would retain the box of cell phones in her possession. However, the box of cell phones was left in the home when AHKTER's mother moved to Texas. Under his conditions of release, AHKTER is not allowed to have access to these phones because they are unmonitored.

11. In addition, Officer Erding saw a desktop computer in AKHTER's residence that had not been reported to her. AKHTER told Officer Erding that the computer belonged to his grandmother. All computers in AHKTER's home that do not belong to AHKTER are required to be password protected, and AHKTER is not allowed to have the password. However, Officer

² AKHTER had previously been living with his mom, dad, sister, and grandmother following his release. However, his mom, dad, and sister have since moved to Texas, leaving him in the custody of his grandmother.

Erding was able to access the computer without a password. The desktop computer supposedly belonging to the grandmother does not have computer monitoring software installed.

12. For the foregoing reasons, the United States submits that there is probable cause to believe that AHKTER in violation of 18 U.S.C. §§ 1343 (Wire Fraud) and 1030(a)(2)(C) (Access of a Protected Computer without Authorization), and that AKHTER is using unmonitored electronic devices to conduct the criminal activity.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

13. As described above and in Attachment B, this application seeks permission to search for records that might be found in the VEHICLE, in whatever form they are found. One form in which the records might be found is data stored on computer hard drives or other storage media, to include peripherals and loose media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

14. *Probable cause.* I submit that if a computer or storage medium is found in the VEHICLE, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

15. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the VEHICLE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatory or exculpatory the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the

chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium

for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

16. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who

has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

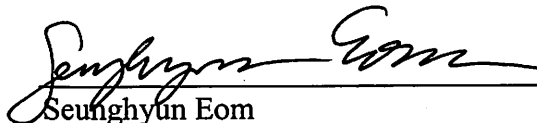
17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying

storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION


18. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,



Seunghyun Eom
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on June 7, 2017:

/s/ 

John F. Anderson
The Honorable John F. Anderson
United States Magistrate Judge
United States Magistrate Judge